

WHAT IS CLAIMED IS:

1. A method for encrypting information using encryption keys, wherein each key encrypts a portion of information of a predetermined block length, the method comprising using a first key to encrypt a first portion of a message; adding at least one bit of information to the encrypted first portion of the message; using a second key to encrypt a second portion of the message wherein the second portion overlaps with the first portion and also includes the added one or more bits of information.